

Healthcare Industry - Glossary of Terms



Background: Providing healthcare in recent years has become a complex, costly endeavor characterized by massive change and constant distractions. Currently, physicians and office administrators are focused on implementing stage 2 of meaningful use of electronic health records, preparing to provide patient access to online medical records, as well as gearing up for ICD-10, which will increase the number of diagnostic codes by 54,000 (up from 14,000 in the current ICD-9-CM code set, which is 30 years old).

ARRA - American Recovery and Reinvestment Act of 2009 is often called the Stimulus or Recovery Act, since its primary purpose was an economic stimulus package in response to the Great Recession. The ARRA is important in the context of this glossary because it included a section known as the HITECH Act.

BA - Business associate is any organization or person working in association with or providing services to a covered entity who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR). Examples include accounting or consulting firms who work with covered entities. Updates made to the HIPAA regulation by the HITECH Act require business associates to comply with HIPAA mandates regarding the handling and use of PHI. As of 2010, HHS can audit business associates for HIPAA compliance and fine them for non-compliance and data breaches.

BAA – As per HIPAA, a business associate agreement is a contract between a HIPAA covered entity and a HIPAA business associate. The contract protects personal health information in accordance with HIPAA guidelines. A BAA should explicitly spell out how a BA will report and respond to a data breach, including those caused by a business associate's subcontractors. BAA should also require a BA to demonstrate how it will respond to an OCR investigation.

Covered Entity - A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most common examples are hospitals, doctors' offices and health insurance providers. Covered entities are required to comply with HIPAA and HITECH mandates for the protection of PHI and PHR.

EHR - Electronic Health Records, a systematic collection of electronic health information about an individual patient or population in a digital format that can be shared across different healthcare settings. EHRs may include demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images,

vital signs, personal statistics like age and weight, and billing information, which may include personal identification data and credit card numbers.

EHR Incentives – EHR is a critical national goal in establishing an electronic health information exchange. The goal goes beyond adoption to the meaningful use of EHRs, such that healthcare providers can achieve significant improvements in care. Incentives for EHR adoption by healthcare providers were established by HIPAA, and relate to Medicaid and Medicare with maximum incentive payments for Medicaid of \$63,750 over 6 years beginning in 2011 and maximum payments for Medicare of \$44,000 over 5 years. Doctors who do not adopt EHR by 2015 will be penalized 1% of Medicare payments, increasing to 3% over 3 years. In order to receive the EHR stimulus money, the HITECH Act requires doctors to show "meaningful use" of an EHR system.

EMR - An electronic medical record (EMR) is a digital version of a paper chart that contains all of a patient's medical history from one practice. An EMR is mostly used by providers for diagnosis and treatment. The information stored in EMRs is not easily shared with providers outside of a practice, and patient records may even have to be printed and mailed to other members of the care team.

ePHI - Electronic protected health information refers to any PHI that is covered under HIPAA security regulations and is produced, saved, transferred or received in an electronic form. There are 18 specific types of ePHI including patient names, addresses, Social Security numbers, email addresses, and fingerprints or photographic images, among others. In addition, any past medical records or payment information is subject to the same degree of privacy protection.

HHS - The United States Department of Health and Human Services (HHS), also known as the Health Department, is a cabinet-level department whose goal is to protect the health of all Americans and provide essential human services. Before the separate federal Department of Education was created in 1979, it was called the Department of Health, Education, and Welfare (HEW).

HIE - Health information exchange is a core capability for hospitals and physicians to achieve "meaningful use" and receive stimulus funding. Healthcare vendors are promoting HIE as a way to allow EHR systems to access disparate data and inter-operate more seamlessly. Starting in 2015, hospitals and doctors will be subject to financial penalties related to Medicare payments if they are not using EHR.

HIPAA - The Health Insurance Portability and Accountability Act of 1996 has also been known as the Kennedy-Kassebaum or Kassebaum-Kennedy Act after its sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health

care transactions and national identifiers for providers, health insurance plans, and employers. AS provisions also address the security and privacy of health data, and its standards are meant to encourage widespread use of electronic data interchange in the U.S. healthcare system.

HIT - Health information technology (health IT) involves the exchange of health information in an electronic environment. Widespread use of health IT within the health care industry will improve the quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care. It is imperative that the privacy and security of electronic health information be ensured as this information is maintained and transmitted electronically.

HITECH Act - Enactment of the Health Information Technology for Economic and Clinical Health Act was a product of ARRA. Of the \$155 billion allocated by ARRA to fund health care spending, \$86.8 billion was for Medicaid and \$25.8 billion was earmarked for health information technology (HIT) investments and incentive payments to adopt EHRs.

ICD - The International Classification of Diseases (ICD) is the standard diagnostic tool for epidemiology, health management and clinical purposes. It is used to analyze and monitor the general health situation of population groups. This set of codes is used to classify diseases and other health problems recorded on many types of health and vital records—such as death certificates and health records—and also provide the basis for the compilation of national mortality and morbidity statistics by World Health Organization member states. ICD-10 was endorsed in 1990 and came into use in 1994. ICD-10 increases the number of diagnostic codes by 54,000 (up from 14,000 in the ICD-9-CM code set, which is 30 years old).

MU - Meaningful Use of electronic health records, as mandated by HIPAA for healthcare providers who accept Medicare or Medicaid payments from the government. The main components of Meaningful Use are (1) use of a certified EHR system in a meaningful manner, such as e-prescribing; (2) use of certified EHR technology for electronic exchange of health information to improve quality of healthcare, and (3) use of certified EHR technology to submit clinical quality and other measures.

OCR – The Office for Civil Rights is the auditing and enforcement arm of HHS. Federal civil rights laws and the HIPAA Privacy Rule together protect Americans from unfair treatment or discrimination due to race, color, national origin, disability, age, gender or religion. The OCR announced in late 2012 that it would strengthen its enforcement among smaller practices and apply penalties for small data breaches.

ONC - The Office of the National Coordinator for Health Information Technology, a staff division within HHS created by Executive Order in 2004 and written into legislation by the HITECH Act. Its purpose is to promote a national health Information Technology infrastructure and oversee its development.

Omnibus Rule - Enacted by HHS OCR to modify the HIPAA Privacy, Security and Enforcement Rules to implement statutory amendments under the HITECH Act. The Omnibus or Final Rule constitutes the most extensive changes to the HIPAA Privacy and Security Rules since they were first implemented in 1996. Among the most significant is the application of PHI protection standards to HIPAA business associates and their subcontractors. Others are modifying the Breach Notification Rule for unsecured PHI with more objective standards for assessing liability following a data breach; increasing penalties for non-compliance based on the level of negligence, with a maximum penalty of \$1.5 million per violation; and prohibiting the sale of an individuals' health information without their permission.

PHI - Protected health information is any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

REC – Regional extension centers, referring to the Health Information Technology Regional Extension Centers (HITREC) established by the HITECH Act as part of the Health Information Technology Extension Program, along with a national Health IT Research Center (HITRC). The RECs offer local technical assistance, guidance, and information to support and accelerate healthcare providers' efforts to implement certified EHR technology and become meaningful users of those systems. These centers were funded originally by grants from the ONC.

Sources for this information include hhs.gov, healthit.gov, whatis.techtarget.com, and Wikipedia websites as of April, 2014. Any errors in interpretation are strictly our own.